

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-131449

(43)Date of publication of application : 19.05.1995

(51)Int. Cl. H04L 9/00
 H04L 9/10
 H04L 9/12
 G06F 13/00
 G09C 1/00

(21)Application number : 05-275386

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 04.11.1993

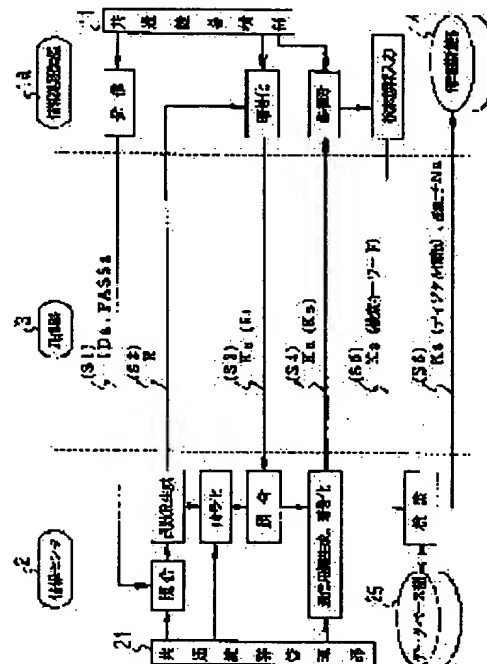
(72)Inventor : YAMANAKA KIYOSHI

(54) DIGITAL INFORMATION COMMUNICATION SYSTEM

(57)Abstract:

PURPOSE: To provide the digital information communication system which protects information from the wrong action like wrong copy or alteration of data.

CONSTITUTION: When information is received from an information center 2 by an information processor 1a and is used, digital information to which an alteration prevention authenticator Na is given is received by communication in the cipher system using a common key Ka; and at, the time of using the information, received digital information is decoded and converted and is outputted only when it passes alteration verification by the authenticator Na. Consequently, essential intended information cannot be restored even if received digital information is copied as it is and is decoded and converted by another device or the like and is outputted, and wrong copy is prevented. Thus, the rights and profits of a writer and an information presenter are protected.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平7-131449

(43)公開日 平成7年(1995)5月19日

(51)Int.Cl. ^a	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/00				
9/10				
9/12				
G 0 6 F 13/00	3 5 1 Z	7368-5B		
			H 0 4 L 9/ 00	Z
			審査請求 未請求 請求項の数4	OL (全 15 頁) 最終頁に続く

(21)出願番号 特願平5-275386

(22)出願日 平成5年(1993)11月4日

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(72) 発明者 山中 喜義

東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

(74)代理人 弁理士 吉田 精孝

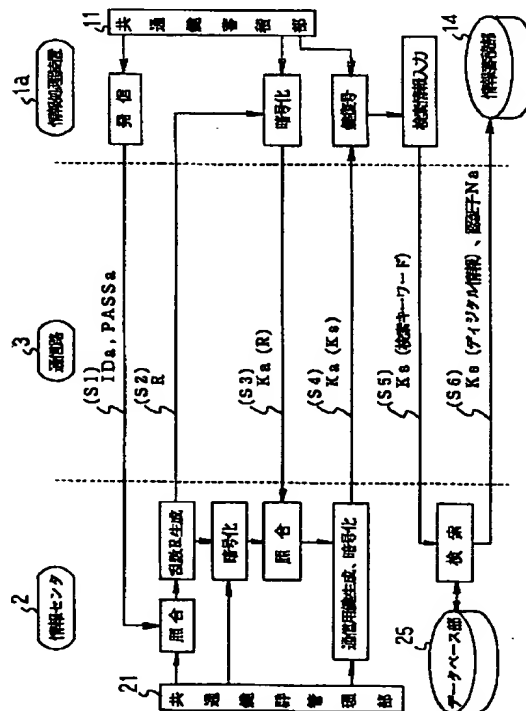
(54) 【発明の名称】 デジタル情報通信システム

(57) 【要約】

【目的】 データの不正コピー、改ざん等の不正行為に対して情報を保護するデジタル情報通信システムを提供すること。

【構成】 情報センタ 2 から情報処理装置 1 a に情報を受信して使用する際に、改ざん防止用認証子 N a を付与したデジタル情報を共通鍵 K a を用いた暗号方式の通信により受信し、利用時に認証子 N a により改ざん検証して適合した場合のみ受信したデジタル情報を復号及び変換して出力する。

【効果】 受信したデジタル情報をそのままコピーして他の装置などで復号、変換出力しても、本来の意図する情報は復元されず、不正コピーを防止できる。これにより著作権並びに情報提供業者の権利及び利益を保護することができる。



【特許請求の範囲】

【請求項 1】 装置番号及びパスワード並びに共通鍵を蓄積する共通鍵蓄積部と、デジタル情報を受信制御する通信制御部と、通信開始時に装置の認証のための認証情報を作成する認証データ作成部と、受信したデジタル情報を蓄積する情報蓄積部と、デジタル情報を復号する復号部と、該復号されたデジタル情報を所定の形態に変換して外部に出力する変換出力部とからなる情報処理装置と、
 複数の情報処理装置に対応する装置番号及びパスワード並びに共通鍵群を蓄積する共通鍵群管理部と、前記情報処理装置にデジタル情報を送信制御する通信制御部と、各情報処理装置から認証情報を受信して接続可否を判定する認証部と、検索用デジタル情報を格納するデータベース部と、該データベース部内のデジタル情報を検索する検索部と、デジタル情報を暗号化する暗号管理部とからなる情報センタとを備え、前記情報処理装置と前記情報センタとの間でデジタル情報通信を行うデジタル情報通信システムであって、
 前記情報センタに格納されているデジタル情報を前記情報処理装置に取り込むときは、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、
 該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を前記情報処理装置に送信し、
 該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、
 該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して前記情報処理装置に送信し、
 暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した検索キーワードを前記情報センタに送信し、
 該検索キーワードを受信した情報センタは、該検索キーワードに基づいて前記データベース部内のデジタル情報を検索し、検索結果のデジタル情報を前記通信用暗号鍵で暗号化すると共に前記情報処理装置に対応した認証子を作成して、これらを前記情報処理装置に返送し、
 前記デジタル情報及び認証子を受信した情報処理装置は、これらを前記情報蓄積部に蓄積した後、認証子の検証及びデジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力することを特徴とするデジタル情報通信システム。

【請求項 2】 前記情報センタのデジタル情報を他の情報処理装置によっても利用することを前提として前記情報処理装置に取り込むときは、

前記暗号化された通信用暗号鍵を前記情報センタから受信した前記情報処理装置は、検索キーワード及びデジタル情報を利用する他の情報処理装置の装置番号を該通信用暗号鍵で暗号化して前記情報センタに送信し、
 該検索キーワード及び他の情報処理装置の装置番号を受信した情報センタは、該検索キーワードに基づいて前記データベース部内のデジタル情報を検索し、検索結果のデジタル情報を前記通信用暗号鍵で暗号化すると共に前記情報処理装置に対応した認証子を作成して、これらを前記情報処理装置に返送すると同時に、前記他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記デジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、
 該他の情報処理装置に対応した通信用暗号鍵及び認証子を受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたデジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、
 該複写先の他の情報処理装置は、前記認証子の検証及びデジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力することを特徴とする請求項 1 記載のデジタル情報通信システム。

【請求項 3】 前記情報センタのデジタル情報を前記情報処理装置に取り込み通信を終了した後、該デジタル情報を他の情報処理装置によって利用するときは、
 前記情報処理装置を再度前記情報センタに接続して、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、
 該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を情報処理装置に送信し、
 該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、
 該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して情報処理装置に送信し、
 暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した前記デジタル情報固有の情報識別番号及び前記他の情報処理装置の装置番号、並びに前記情報処理装置の共通鍵で暗号化した前記デジタル情報受信時に使用した通信用暗号鍵を前記情報センタに送信し、
 前記情報識別番号及び装置番号並びに通信用暗号鍵を受信した情報センタは、前記他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記デジタル情

報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、

該他の情報処理装置に対応した通信用暗号鍵及び認証子を受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたデジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、該複写先の他の情報処理装置は、前記認証子の検証及びデジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力することを特徴とする請求項 1 記載のデジタル情報通信システム。

【請求項 4】 前記他の情報処理装置に蓄積されている前記情報センタから受信したデジタル情報を前記情報処理装置によって利用するときは、前記情報処理装置を情報センタに接続して、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を前記情報処理装置に送信し、該乱数を受信した前記情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して前記情報処理装置に送信し、暗号化された通信用暗号鍵を受信した前記情報処理装置は、該通信用暗号鍵で暗号化した前記他の情報処理装置で受信したデジタル情報固有の情報識別番号、及び前記他の情報処理装置の共通鍵で暗号化した前記デジタル情報受信時に使用した通信用暗号鍵、並びに該通信用暗号鍵で暗号化した前記他の情報処理装置の装置番号を前記情報センタに送信し、前記情報識別番号及び装置番号並びに通信用暗号鍵を受信した情報センタは、前記情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記デジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、該通信用暗号鍵及び認証子を受信した情報処理装置側では、前記他の情報処理装置から前記情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたデジタル情報を複写し、該デジタル情報が複写された前記情報処理装置は、前記認証子の検証及び前記デジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力することを特徴とする請求項 1 記載のデジタル情報通信システム。

ム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、音楽、映像、絵画、コンピュータグラフィックス、コンピュータソフトウェア等の著作物情報を ISDN 等の通信回線によりデジタル情報として送信する際、通信に先立つ送信先の認証、通信途中での盗聴防止、並びに受信後の情報の改ざん及び不正コピーを防止し、且つ複数装置で利用を可能とする合法的コピーを許容することにより、著作権者並びに情報提供者の権利及び利益を保護するデジタル情報通信システムに関するものである。

【0002】

【従来の技術】近年、ISDN を代表とするデジタル通信技術及び、デジタル情報圧縮技術（例えば、MPEG, JPEG 方式等）の発達により、音楽、絵画、映像、コンピュータソフト、コンピュータグラフィックス等の著作物をデジタル情報として通信回線利用により送信することが実現可能となってきた。例えば、コンピュータソフトウェアでは、既にパソコン通信等を利用した配送サービスを実施している例がある。今後は早晩、さらに情報量の多い音楽、映像情報等の配送サービスの出現が予想される。

【0003】

【発明が解決しようとする課題】前述したように、デジタル著作物の通信利用による流通が盛んになると、デジタル情報の送信相手になりすまして通信を行ったり、或いは通信途中での盗聴等に加えて、受信した情報をデジタル形式で不正に複製して他の装置で利用する不正行為により著作権者並びに情報提供業者の権利及び利益を侵害する恐れが生じる。

【0004】従来のパソコン通信利用によるコンピュータソフトウェア配送では、情報提供元となるセンタと接続する時に、ユーザ ID、パスワードによる簡易な相手確認を行う程度で通信途中での盗聴、受信後のデータの不正コピー、改ざん等の不正行為に対して防止対策が施されていなかった。

【0005】一方、従来の不正コピー防止対策としては、フロッピーディスクの場合、標準記録方式（記録密度、セクタ、トラック数等）から一部逸脱した記録方式で記録する等して、一般のコピープログラムではリードエラーが発生する仕組みを設けている例がある。しかし、この方式では、フロッピーディスク等の記憶媒体の物理的破壊防止のためのバックアップコピーを行うことが困難になってしまう。

【0006】また、デジタル情報の通信利用による配送の場合、通信の効率化及び利用者拡大を図るため、著作権者並びに情報提供者の権利を保護しつつ、合法的コピーを許容して、一度受信したデジタル情報を複数利用者、複数装置で利用できる仕組みは、従来のフロッピー

ディスクのコピープロテクト方式では困難であった。

【0007】本発明の目的は上記の問題点に鑑み、データの不正コピー、改ざん等の不正行為に対して情報を保護するデジタル情報通信システムを提供することにある。

【0008】

【課題を解決するための手段】本発明は上記の目的を達成するために、請求項1では、装置番号及びパスワード並びに共通鍵を蓄積する共通鍵蓄積部と、デジタル情報を受信制御する通信制御部と、通信開始時に装置の認証のための認証情報を作成する認証データ作成部と、受信したデジタル情報を蓄積する情報蓄積部と、デジタル情報を復号する復号部と、該復号されたデジタル情報を所定の形態に変換して外部に出力する変換出力部とからなる情報処理装置と、複数の情報処理装置に対応する装置番号及びパスワード並びに共通鍵群を蓄積する共通鍵群管理部と、前記情報処理装置にデジタル情報を送信制御する通信制御部と、各情報処理装置から認証情報を受信して接続可否を判定する認証部と、検索用デジタル情報を格納するデータベース部と、該データベース部内のデジタル情報を検索する検索部と、デジタル情報を暗号化する暗号管理部とからなる情報センタとを備え、前記情報処理装置と前記情報センタとの間でデジタル情報通信を行うデジタル情報通信システムであって、前記情報センタに格納されているデジタル情報を前記情報処理装置に取り込むときは、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を前記情報処理装置に送信し、該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して前記情報処理装置に送信し、暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した検索キーワードを前記情報センタに送信し、該検索キーワードを受信した情報センタは、該検索キーワードに基づいて前記データベース部内のデジタル情報を検索し、検索結果のデジタル情報を前記通信用暗号鍵で暗号化すると共に前記情報処理装置に対応した認証子を作成して、これらを前記情報処理装置に返送し、前記デジタル情報及び認証子を受信した情報処理装置は、これらを前記情報蓄積部に蓄積した後、認証子の検証及びデジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力するデジタル情報通信システムを

提案する。

【0009】また、請求項2では、請求項1記載のデジタル通信システムにおいて、前記情報センタのデジタル情報を他の情報処理装置によっても利用することを前提として前記情報処理装置に取り込むときは、前記暗号化された通信用暗号鍵を前記情報センタから受信した前記情報処理装置は、検索キーワード及びデジタル情報を利用する他の情報処理装置の装置番号を該通信用暗号鍵で暗号化して前記情報センタに送信し、該検索キーワード及び他の情報処理装置の装置番号を受信した情報センタは、該検索キーワードに基づいて前記データベース部内のデジタル情報を検索し、検索結果のデジタル情報を前記通信用暗号鍵で暗号化すると共に前記情報処理装置に対応した認証子を作成して、これらを前記情報処理装置に返送すると同時に、前記他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記デジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、該他の情報処理装置に対応した通信用暗号鍵及び認証子を受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたデジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、該複写先の他の情報処理装置は、前記認証子の検証及びデジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力するデジタル情報通信システムを提案する。

【0010】また、請求項3では、請求項1記載のデジタル通信システムにおいて、前記情報センタのデジタル情報を前記情報処理装置に取り込み通信を終了した後、該デジタル情報を他の情報処理装置によって利用するときは、前記情報処理装置を再度前記情報センタに接続して、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を情報処理装置に送信し、該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して情報処理装置に送信し、暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した前記デジタル情報固有の情報識別番号及び前記他の情報処理装置の装置番号、並びに前記情報処理装置の共通鍵で暗号化した前記デジタル情報受信時に使用した通信用暗号鍵を前記情報センタに送信し、

前記情報識別番号及び装置番号並びに通信用暗号鍵を受信した情報センタは、前記他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記デジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、該他の情報処理装置に対応した通信用暗号鍵及び認証子を受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたデジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、該複写先の他の情報処理装置は、前記認証子の検証及びデジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力するデジタル情報通信システムを提案する。

【0011】さらに、請求項4では、請求項1記載のデジタル通信システムにおいて、前記他の情報処理装置に蓄積されている前記情報センタから受信したデジタル情報を前記情報処理装置によって利用するときは、前記情報処理装置を情報センタに接続して、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を前記情報処理装置に送信し、該乱数を受信した前記情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して前記情報処理装置に送信し、暗号化された通信用暗号鍵を受信した前記情報処理装置は、該通信用暗号鍵で暗号化した前記他の情報処理装置で受信したデジタル情報固有の情報識別番号、及び前記他の情報処理装置の共通鍵で暗号化した前記デジタル情報受信時に使用した通信用暗号鍵、並びに該通信用暗号鍵で暗号化した前記他の情報処理装置の装置番号を前記情報センタに送信し、前記情報識別番号及び装置番号並びに通信用暗号鍵を受信した情報センタは、前記情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記デジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、該通信用暗号鍵及び認証子を受信した情報処理装置側では、前記他の情報処理装置から前記情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたデジタル情報を複写し、該デジタル情報が複写された前記情報処理装置は、前記認証子の検証及び前記デジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力するデジタル情報通信システムを提案する。

【0012】

【作用】本発明の請求項1によれば、前記情報センタのデジタル情報を前記情報処理装置に取り込むときは、前記情報処理装置から前記情報センタに装置番号及びパスワードが送信され、該装置番号及びパスワードを受信した情報センタにおいて、乱数が生成され、該乱数が前記情報処理装置に送信される。該乱数を受信すると、前記情報処理装置は該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、前記情報センタにおいて、前記情報処理装置に対応した共通鍵が前記共通鍵群管理部から抽出されると共に、該共通鍵により前記送信時の乱数が暗号化され、該暗号化された乱数と前記情報処理装置から受信した暗号化された乱数とが比較され、これらの値が一致したときに、通信用暗号鍵が作成されると共に該通信用暗号鍵が前記共通鍵で暗号化されて前記情報処理装置に送信される。

【0013】暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した検索キーワードを情報センタに送信する。これにより情報センタでは、該検索キーワードに基づいて前記データベース部内のデジタル情報が検索され、検索結果のデジタル情報が前記通信用暗号鍵で暗号化されると共に前記情報処理装置に対応した認証子が作成されて、これらの情報処理装置に返送される。

【0014】前記情報処理装置は前記情報センタからデジタル情報及び認証子を受信した後、これらを前記情報蓄積部に蓄積し、認証子の検証及びデジタル情報の復号を行ってから、情報内容に応じた利用形態に変換して出力する。

【0015】また、請求項2によれば、前記情報センタのデジタル情報を他の情報処理装置によっても利用することを前提として前記情報処理装置に取り込む際に、前記暗号化された通信用暗号鍵を前記情報センタから受信した情報処理装置は、検索キーワード及びデジタル情報を利用する他の情報処理装置の装置番号を該通信用暗号鍵で暗号化して情報センタに送信する。これにより、該検索キーワード及び他の情報処理装置の装置番号を受信した情報センタでは、該検索キーワードに基づいて前記データベース部内のデジタル情報が検索され、検索結果のデジタル情報が前記通信用暗号鍵によって暗号化されると共に前記情報処理装置に対応した認証子が作成されて、これらの前記情報処理装置に返送される。さらにこれと同時に、前記情報センタから前記情報処理装置に対して、前記他の情報処理装置に対応する共通鍵によって暗号化された通信用暗号鍵と前記デジタル情報に対して該共通鍵により作成された認証子が送信される。

【0016】この後、前記情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前

記受信した通信用暗号鍵で暗号化されたデジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、該複写先の他の情報処理装置は、前記認証子の検証及びデジタル情報の復号を行ってから、情報内容に応じた利用形態に変換して出力する。

【0017】また、請求項3によれば、前記情報センタのデジタル情報を前記情報処理装置に取り込み通信を終了した後、該デジタル情報を他の情報処理装置によって利用する際に、前記情報処理装置が再度前記情報センタに接続されて、前記情報処理装置から前記情報センタに装置番号及びパスワードが送信される。これにより、前記情報センタでは、乱数が生成され、該乱数が前記情報処理装置に送信される。該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信する。該暗号化した乱数を受信した情報センタでは、前記情報処理装置に対応した共通鍵が前記共通鍵群管理部から抽出されると共に、該共通鍵により前記送信時の乱数が暗号化され、該暗号化された乱数と前記情報処理装置から受信した暗号化された乱数とが比較され、これらの値が一致したときに、通信用暗号鍵が作成されると共に該通信用暗号鍵が前記共通鍵で暗号化されて前記情報処理装置に送信される。

【0018】この後、前記情報処理装置は、該通信用暗号鍵で暗号化した前記デジタル情報固有の情報識別番号及び前記他の情報処理装置の装置番号、並びに前記情報処理装置の共通鍵で暗号化した前記デジタル情報受信時に使用した通信用暗号鍵を前記情報センタに送信する。次いで、情報センタによって、前記他の情報処理装置に対応する共通鍵によって暗号化された通信用暗号鍵と、前記デジタル情報に対して該共通鍵により作成された認証子が前記情報処理装置に送信される。これらを受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に対して、前記受信した通信用暗号鍵で暗号化されたデジタル情報及び他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、該複写先の他の情報処理装置では、前記認証子の検証及びデジタル情報の復号が行われ、この後情報内容に応じた利用形態に変換されて出力される。

【0019】さらに、請求項4によれば、前記他の情報処理装置に蓄積されている前記情報センタから受信したデジタル情報を前記情報処理装置によって利用する際は、前記情報処理装置が情報センタに接続され、前記情報処理装置から前記情報センタに装置番号及びパスワードが送信される。これにより情報センタでは、乱数が生成され、該乱数が前記情報処理装置に送信される。さらに、該乱数を受信した前記情報処理装置によって、該乱数が前記共通鍵蓄積部より抽出した共通鍵により暗号化

された値が再び前記情報センタに送信される。

【0020】この後、前記情報センタによって、前記情報処理装置に対応した共通鍵が前記共通鍵群管理部から抽出されると共に、該共通鍵により前記送信時の乱数が暗号化され、該暗号化された乱数と前記情報処理装置から受信した暗号化された乱数とが比較され、これらの値が一致したときに、通信用暗号鍵が作成されると共に該通信用暗号鍵が前記共通鍵によって暗号化されて前記情報処理装置に送信される。次いで、前記情報処理装置によって、該通信用暗号鍵で暗号化された前記他の情報処理装置で受信したデジタル情報固有の情報識別番号、及び前記他の情報処理装置の共通鍵で暗号化した前記デジタル情報受信時に使用した通信用暗号鍵、並びに該通信用暗号鍵で暗号化した前記他の情報処理装置の装置番号が情報センタに送信される。

【0021】これらを受信した情報センタでは、前記情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記デジタル情報に対して該共通鍵により作成された認証子が前記情報処理装置に送信され、該通信用暗号鍵及び認証子を受信した情報処理装置側では、前記他の情報処理装置から前記情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたデジタル情報を複写し、該デジタル情報が複写された情報処理装置は、前記認証子の検証及びデジタル情報の復号を行ってから、情報内容に応じた利用形態に変換して出力する。

【0022】

【実施例】以下、図面に基づいて本発明の一実施例を説明する。図1は、本発明の一実施例に係るデジタル情報通信システムを示す構成図である。図において、1はデジタル情報を受信し、これを蓄積して利用する情報処理装置、2はデジタル情報の提供元となる情報センタで、デジタル情報を蓄積し、情報処理装置1からの検索要求によりデジタル情報を送信する。3は通信路で、該通信路3を介して情報センタ2と複数の情報処理装置1とが接続できるようになっている。

【0023】情報処理装置1は、装置番号及びパスワード並びに共通鍵を蓄積する共通鍵蓄積部11、デジタル情報を受信制御する通信制御部12、通信開始時に装置の認証のための認証情報を作成する認証データ作成部13、受信したデジタル情報を蓄積する情報蓄積部14、デジタル情報を復号する復号部15、及び復号されたデジタル情報を外部に例えばアナログ情報として変換出力する変換出力部16を備え、これらはキーボード等からなる入力インタフェース部（図示せず）に接続された図示せぬ中央制御部によって動作制御されている。

【0024】情報センタ2は、複数の情報処理装置1に対応する装置番号及びパスワード並びに共通鍵群を蓄積する共通鍵群管理部21、情報処理装置1へのディジタ

ル情報の送信を制御する通信制御部 2 2、各情報処理装置 1 から認証情報を受信して接続可否を判定する認証部 2 3、デジタル情報を検索する検索部 2 4、検索用デジタル情報を格納するデータベース部 2 5、デジタル情報を暗号化する暗号化部 2 6 から構成され、これらは図示せぬ中央制御部によって動作制御されている。

【0025】図 2 は、情報処理装置 1 内の共通鍵蓄積部 1 1 に蓄積される情報の内容例を示す図である。図において、IDa は装置番号、PASSa はパスワード、Ka は共通鍵である。

【0026】図 3 は、情報センタ 2 内の共通鍵群管理部 2 1 に蓄積される情報の内容例を示す図である。図において、IDa ~ IDc、PASSa ~ PASSc、Ka ~ Kc のそれぞれは、異なる情報処理装置 1 a、1 b、1 c の装置番号、パスワード、共通鍵を示している。

【0027】本実施例の処理の流れを情報処理装置 1 a と情報センタ 2 の間での通信を例として、図 1 及び図 4 に基づいて説明する。ここで、情報処理装置 1 a の構成は図 1 に示す情報処理装置 1 の構成と同等である。

【0028】情報処理装置 1 a は情報センタ 2 に発信して、共通鍵蓄積部 1 1 より抽出した情報処理装置 1 a の装置番号 IDa 及びパスワード PASSa を情報センタ 2 に送信する (S1)。情報センタ 2 では、前記受信した装置番号 IDa 及びパスワード PASSa を共通鍵群管理部 2 1 で検索し、該装置番号 IDa 及びパスワード PASSa が存在し且つこれらの組み合わせが一致した場合に、乱数 R を生成して情報処理装置 1 a に返送する (S2)。

【0029】情報処理装置 1 a は、乱数 R を受信した後、認証データ作成部 1 3 において受信した乱数 R を共通鍵蓄積部 1 1 より抽出した共通鍵 Ka によって暗号化し、暗号化した乱数 Ka (R) を情報センタ 2 に送信する (S3)。

【0030】情報センタ 2 では、認証部 2 3 において、共通鍵群管理部 2 1 より抽出した情報処理装置 1 a に対応する共通鍵 Ka で前記乱数 R を暗号化すると共に、該暗号化した乱数 R の値と受信した暗号化乱数 Ka (R) の値とを照合する。この照合の結果、両者の値が一致した場合には、通信用暗号鍵 Ks を生成すると共に、該通信用暗号鍵 Ks を情報処理装置 1 a に対応する共通鍵 Ka で暗号化し、暗号化した通信用暗号鍵 Ka (Ks) を情報処理装置 1 a に送信する (S4)。

【0031】次に、情報処理装置 1 a は暗号化した通信用暗号鍵 Ka (Ks) を受信した後、これを復号して通信用暗号鍵 Ks を復元し、検索したいデジタル情報に対応する検索キーワードを前記通信用暗号鍵 Ks で暗号化して情報センタ 2 に送信する (S5)。

【0032】情報センタ 2 では、情報処理装置 1 a から検索キーワードを受信すると、検索部 2 4 によって、受信した検索キーワードに対応するデジタル情報をデー

タベース部 2 5 から検索し、暗号化部 2 6 によって、検索抽出したデジタル情報を前記通信用暗号鍵 Ks で暗号化し、さらに認証子 Na を計算して付与した後、これらを情報処理装置 1 a に送信する (S6)。

【0033】情報処理装置 1 a は、受信したデジタル情報並びに認証子 Na を情報蓄積部 1 4 に蓄積する。ここで、認証子 Na は、受信されたデジタル情報の内容の改ざんを検出するためのチェックデータであり、通信用暗号鍵 Ks で暗号化されたデジタル情報に対して例えば MAC (詳細は、ISO 9797 参照) 等のデータ改ざん検出用認証子作成方法により情報センタ 2 で計算して付与される。この時、認証子 Na の作成用鍵として共通鍵 Ka が用いられているので、本情報処理装置の操作者が改ざんを検出されない様に情報内容を変更することは困難となる。

【0034】情報処理装置 1 a の操作者が情報を利用する際には、情報処理装置 1 a 内において利用対象となるデジタル情報の認証子 Na' が計算され、該認証子 Na' と情報センタ 2 から直接受信した認証子 Na とが比較される。この比較の結果、両者が一致した場合にのみ、情報処理装置 1 a の復号部 1 5 で、前記デジタル情報を復号し、変換出力部 1 6 で情報内容に応じた形態に変換して出力が行われる。

【0035】前述のように、共通暗号鍵方式を用いた認証、及び暗号化したデジタル情報の通信を行うことにより、通信相手の特定が可能になると共に、通信途中での盗聴防止が可能となる。さらに、情報処理装置 1 a において受信したデジタル情報を情報蓄積部 1 4 からそのままコピーして他の装置等で復号及び変換出力しても、本来の意図する情報は復元されないの、不正コピーを防止することができる。また、受信したデジタル情報に認証子 Na を付与しているの、受信情報を改ざんした場合、共通鍵 Ka を知らない限り、利用時の検証で改ざん検出がなされ、情報を復号して変換出力することができず改ざん防止が可能となる。これにより、著作権者並びに情報提供者の権利及び利益を保護することができる。

【0036】次に、情報処理装置 1 a において一度受信したデジタル情報を複数の情報処理装置で利用する場合の手順を図 5 及び図 6 に基づいて説明する。図 5 は、情報処理装置 1 a によってデジタル情報を受信する時に、他の情報処理装置 1 b、1 c でも利用することを前提に通信する例を示している。

【0037】まず、情報処理装置 1 a 側では、前述したと同様の手順により情報センタ 2 により認証を受けると共に、通信用暗号鍵 Ks の受信を行う。

【0038】即ち、情報処理装置 1 a 側から情報センタ 2 に発信して、共通鍵蓄積部 1 1 より抽出した情報処理装置 1 a の装置番号 IDa 及びパスワード PASSa を情報センタ 2 に送信する (SP1)。情報センタ 2 で

は、前記受信した装置番号 I D a 及びパスワード P A S S a を共通鍵群管理部 2 1 で検索し、該装置番号 I D a 及びパスワード P A S S a が存在し且つこれらの組み合わせが一致した場合に、乱数 R を生成して情報処理装置 1 a に返送する (S P 2)。

【0039】情報処理装置 1 a は、乱数 R を受信した後、認証データ作成部 1 3 において受信した乱数 R を共通鍵蓄積部 1 1 より抽出した共通鍵 K a によって暗号化し、暗号化した乱数 K a (R) を情報センタ 2 に送信する (S P 3)。

【0040】情報センタ 2 では、認証部 2 3 において、共通鍵群管理部 2 1 より抽出した情報処理装置 1 a に対応する共通鍵 K a で前記乱数 R を暗号化すると共に、該暗号化した乱数 R の値と受信した暗号化乱数 K a (R) の値とを照合する。この照合の結果、両者の値が一致した場合には、通信用暗号鍵 K s を生成すると共に、該通信用暗号鍵 K s を情報処理装置 1 a に対応する共通鍵 K a で暗号化し、暗号化した通信用暗号鍵 K a (K s) を情報処理装置 1 a に送信する (S P 4)。

【0041】次に、情報処理装置 1 a は暗号化した通信用暗号鍵 K a (K s) を受信した後、これを復号して通信用暗号鍵 K s を復元する。この後、情報処理装置 1 a から検索したいデジタル情報に対応する検索キーワード、及び情報を利用したい他の情報処理装置 1 b, 1 c の装置番号 I D b, I D c を前記通信用暗号鍵 K s で暗号化して情報センタ 2 に送信する (S P 5)。

【0042】情報センタ 2 では、情報処理装置 1 a から検索キーワード及び装置番号 I D b, I D c を受信すると、検索部 2 4 によって、受信した検索キーワードに対応するデジタル情報をデータベース部 2 5 から検索して、暗号化部 2 6 によって前記通信用暗号鍵 K s で暗号化し、さらに認証子 N a を計算して付与した後、これらを情報処理装置 1 a に送信する (S P 6)。

【0043】次いで、情報センタ 2 では、先に情報処理装置 1 a から受信した装置番号 I D b, I D c に対応する共通鍵 K b, K c によってそれぞれ暗号化した前記通信用暗号鍵 K s と、共通鍵 K b, K c で作成した認証子 N b, N c とを組合わせて情報処理装置 1 a に送信する (S P 7)。

【0044】情報処理装置 1 a 側では、前記受信した通信用暗号鍵 K s で暗号化されたデジタル情報、並びに各情報処理装置 1 b, 1 c に対応する共通鍵 K b, K c で暗号化された通信用暗号鍵 K b (K s), K c (K s) 及び認証子 N b, N c を対応する情報処理装置 1 b, 1 c の情報蓄積部 1 4 に複写する (S P 8)。

【0045】このときの複写方法は、情報処理装置 1 a と他の情報処理装置 1 b, 1 c とをケーブル接続してダウンロードする方法、またはフロッピーディスク、光ディスク等のパッケージ媒体経由で複写する方法等がある。複写先の情報処理装置 1 b, 1 c でのデジタル情

報の復号並びに変換出力の手順は、先に説明した情報処理装置 1 a での方式と同様である。

【0046】次に、情報処理装置 1 a の単独利用として受信し、情報処理装置 1 a の情報蓄積部 1 4 に蓄積されているデジタル情報を、他の情報処理装置 1 b, 1 c で利用するための情報処理装置 1 a と情報センタ 2 との間の通信及び操作手順を図 6 に基づいて説明する。

【0047】まず、情報処理装置 1 a 側では、前述したと同様の手順により情報センタ 2 により認証を受けると共に、通信用暗号鍵 K s' の受信を行う。

【0048】即ち、情報処理装置 1 a 側から情報センタ 2 に発信して、共通鍵蓄積部 1 1 より抽出した情報処理装置 1 a の装置番号 I D a 及びパスワード P A S S a を情報センタ 2 に送信する (S Q 1)。情報センタ 2 では、前記受信した装置番号 I D a 及びパスワード P A S S a を共通鍵群管理部 2 1 で検索し、該装置番号 I D a 及びパスワード P A S S a が存在し且つこれらの組み合わせが一致した場合に、乱数 R を生成して情報処理装置 1 a に返送する (S Q 2)。

【0049】情報処理装置 1 a は、乱数 R を受信した後、認証データ作成部 1 3 において受信した乱数 R を共通鍵蓄積部 1 1 より抽出した共通鍵 K a によって暗号化し、暗号化した乱数 K a (R) を情報センタ 2 に送信する (S Q 3)。

【0050】情報センタ 2 では、認証部 2 3 において、共通鍵群管理部 2 1 より抽出した情報処理装置 1 a に対応する共通鍵 K a で前記乱数 R を暗号化すると共に、該暗号化した乱数 R の値と受信した暗号化乱数 K a (R) の値とを照合する。この照合の結果、両者の値が一致した場合には、通信用暗号鍵 K s' を生成すると共に、該通信用暗号鍵 K s' を情報処理装置 1 a に対応する共通鍵 K a で暗号化し、暗号化した通信用暗号鍵 K a (K s') を情報処理装置 1 a に送信する (S Q 4)。

【0051】次に、情報処理装置 1 a は暗号化した通信用暗号鍵 K a (K s') を受信した後、これを復号して通信用暗号鍵 K s' を復元する。この後、情報処理装置 1 a によって先に検索したデジタル情報を一意に同定する情報識別番号及び、情報を利用したい他の情報処理装置 1 b, 1 c の装置番号 I D b, I D c を通信用暗号鍵 K s' で暗号化し、さらに、先の通信で使用した通信用暗号鍵 K s を情報処理装置 1 a の共通鍵 K a で暗号化した結果を情報センタ 2 に送信する (S Q 5)。

【0052】この結果、情報センタ 2 は、先に送信した装置番号 I D b, I D c に対応する共通鍵 K b, K c でそれぞれ暗号化した前記通信用暗号鍵 K s と、共通鍵 K b, K c で作成した認証子 N b, N c との組み合わせを情報処理装置 1 a に送信する (S Q 6)。

【0053】次いで、情報処理装置 1 a 側では、先に受信した通信用暗号鍵 K s で暗号化されたデジタル情報と、今回受信した各情報処理装置 1 b, 1 c に対応する

共通鍵 K_b 、 K_c で暗号化された通信用暗号鍵 K_b (K_s)、 K_c (K_s)、及び認証子 N_b 、 N_c を、対応する情報処理装置 1 b、1 c の情報蓄積部 14 に複写する (S Q 7)。

【0054】このときの複写方法も前述と同様であり、複写先の情報処理装置 1 b、1 c でのデジタル情報の復号並びに変換出力の手順は、先に説明した情報処理装置 1 a での方式と同様である。

【0055】次に、情報処理装置 1 a の単独利用として受信し、情報処理装置 1 a の情報蓄積部 14 に蓄積されているデジタル情報を、他の情報処理装置 1 b で利用する際の、情報処理装置 1 b と情報センタ 2 との間の通信及び操作手順を図 7 に基づいて説明する。

【0056】まず、情報処理装置 1 a で受信した暗号化されているデジタル情報を情報処理装置 1 b の情報蓄積部 14 に複写する (S R 1)。この後、情報処理装置 1 b を情報センタ 2 に接続して、前述したと同様の手順により情報センタ 2 により認証を受けると共に、通信用暗号鍵 K_s' の受信を行う。

【0057】即ち、情報処理装置 1 b 側から情報センタ 2 に発信して、共通鍵蓄積部 11 より抽出した情報処理装置 1 b の装置番号 ID_b 及びパスワード $PASS_b$ を情報センタ 2 に送信する (S R 2)。情報センタ 2 では、前記受信した装置番号 ID_b 及びパスワード $PASS_b$ を共通鍵群管理部 21 で検索し、該装置番号 ID_b 及びパスワード $PASS_b$ が存在し且つこれらの組み合わせが一致した場合に、乱数 R を生成して情報処理装置 1 b に返送する (S R 3)。

【0058】情報処理装置 1 b は、乱数 R を受信した後、認証データ作成部 13 において受信した乱数 R を共通鍵蓄積部 11 より抽出した共通鍵 K_b によって暗号化し、暗号化した乱数 $K_b(R)$ を情報センタ 2 に送信する (S R 4)。

【0059】情報センタ 2 では、認証部 23 において、共通鍵群管理部 21 より抽出した情報処理装置 1 b に対応する共通鍵 K_b で前記乱数 R を暗号化すると共に、該暗号化した乱数 R の値と受信した暗号化乱数 $K_b(R)$ の値とを照合する。この照合の結果、両者の値が一致した場合には、通信用暗号鍵 K_s' を生成すると共に、該通信用暗号鍵 K_s' を情報処理装置 1 b に対応する共通鍵 K_b で暗号化し、暗号化した通信用暗号鍵 $K_b(K_s')$ を情報処理装置 1 b に送信する (S R 5)。

【0060】次に、情報処理装置 1 b は暗号化した通信用暗号鍵 $K_b(K_s')$ を受信した後、これを復号して通信用暗号鍵 K_s' を復元する。この後、情報処理装置 1 a によって先に検索したデジタル情報を一意に同定する情報識別番号と情報処理装置 1 a の装置番号 ID_a とを該通信用暗号鍵 K_s' で暗号化すると共に、情報処理装置 1 a で受信した先の通信で使用した通信用暗号鍵 K_s を情報処理装置 1 a の共通鍵 K_a で暗号化し、これ

らの値 K_s' (情報識別番号)、 K_s' (ID_a)、 $K_a(K_s)$ を情報センタ 2 に送信する (S R 6)。

【0061】この結果、情報センタ 2 は、情報処理装置 1 b の共通鍵 K_b で暗号化した前記通信用暗号鍵 K_s と共通鍵 K_b で作成した認証子 N_b を情報処理装置 1 b に送信する (S R 7)。これにより、情報処理装置 1 b において情報処理装置 1 a が受信したデジタル情報を使用することができる。

【0062】前述したように、改ざん防止用認証子を付与したデジタル情報を共通鍵暗号方式での暗号通信により受信し、利用時に認証子による改ざん検証して適合した場合のみ復号、変換して出力しているので、受信したデジタル情報をそのままコピーして他の装置等で復号、変換出力しても、本来の意図する情報は復元されず、不正コピーを防止することができる。

【0063】また、一度受信したデジタル情報を複数利用者の異なる装置で利用したい場合、複数の装置固有の共通鍵で暗号化した通信用鍵および認証子情報のみを受信し、情報量の多いデジタル情報本体を複製して合法的に利用することができるので、著作者、情報提供業者の権利、利益を損なうことがないと共に、情報量の膨大なデジタル情報を利用する情報処理装置の数だけ繰り返して通信する必要がなく、通信コストの低減及び利用者数の拡大を図ることができる。

【0064】

【発明の効果】以上説明したように本発明の請求項 1 によれば、共通鍵暗号方式で通信相手を確認し、認証子付きのデジタル情報を暗号通信により授受し、利用時に認証子を検証して適合した場合のみ復号、変換出力しているため、通信相手の確実な同定、通信途中での盗聴防止が可能となる。さらに、受信したデジタル情報をそのままコピーして他の装置等で復号、変換出力しても、本来の意図する情報は復元されず、不正コピーを防止できる。また、受信情報に認証子を付与することにより、受信情報を改ざんした場合も、共通鍵を知らない限り、利用時の検証により改ざん検出し、復号、変換出力しない機構になっており、改ざん防止も可能となる。また、デジタル情報蓄積部に蓄積された受信情報をそのままコピーして保存しておき、利用時に再度同一のデジタル情報処理装置のデジタル情報蓄積部に戻してから、復号、変換出力して利用することができるため、デジタル情報蓄積部の蓄積容量制限以上に受信しても外部記憶装置に保存しておくことができる。また、デジタル情報蓄積部のファイルの人為的でない物理的破壊等に備えてのバックアップコピーとしても機能するという大きな効果がある。これらの結果、著作者及び情報提供業者の権利並びに利益を保護することができる。

【0065】また、請求項 2 によれば、上記の効果に加えて、一度受信したデジタル情報を他の複数の情報処理装置での合法的利用が可能になり、情報量の膨大なデ

ィジタル情報を利用する情報処理装置の数だけ繰り返して通信する必要がなく、通信コストの低減及び利用者数の拡大を図ることができ、この結果、著作者及び情報提供業者の権利保護並びに利益拡大に貢献することができる。

【0066】また、請求項3によれば、上記の効果に加えて、任意の情報処理装置によって受信したデジタル情報を必要時に応じて他の情報処理装置で使用することができる。

【0067】さらに、請求項4によれば、上記の効果に加えて、任意の情報処理装置によって受信したデジタル情報を他の情報処理装置で使用する際に、該他の情報処理装置と情報センタとの通信によって、該他の情報処理装置において前記デジタル情報を合法的に使用することができ、利用手続の簡単化を図ることができるという非常に優れた効果を奏するものである。

【図面の簡単な説明】

【図1】本発明の一実施例におけるディジタル情報通信システムを示す構成図

【図2】一実施例における共通鍵蓄積部内の情報内容例を示す図

【図2】

IDa	PASSa	Ka
-----	-------	----

【図3】一実施例における共通鍵群管理部内の情報内容例を示す図

【図4】一実施例における情報処理装置と情報センタとの間での通信手順を説明する図

【図5】一実施例における情報処理装置と情報センタとの間での通信手順及び他の情報処理装置への複写手順を説明する図

【図6】一実施例における情報処理装置と情報センタとの間での通信手順及び他の情報処理装置への複写手順を説明する図

【図7】一実施例における情報処理装置と情報センタとの間での通信手順及び他の情報処理装置への複写手順を説明する図

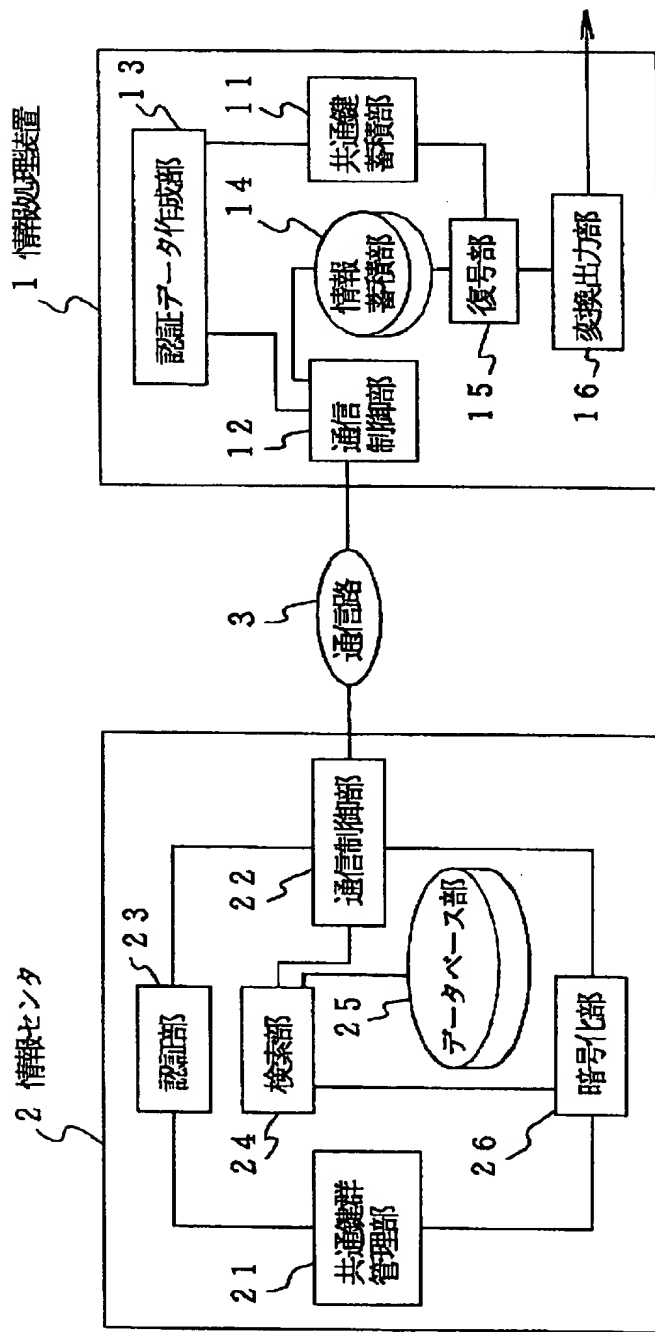
【符号の説明】

1…情報処理装置、11…共通鍵蓄積部、12…通信制御部、13…認証データ作成部、14…情報蓄積部、15…復号部、16…変換出力部、2…情報センタ、21…共通鍵群管理部、22…通信制御部、23…認証部、24…検索部、25…データベース部、26…暗号化部、3…通信路。

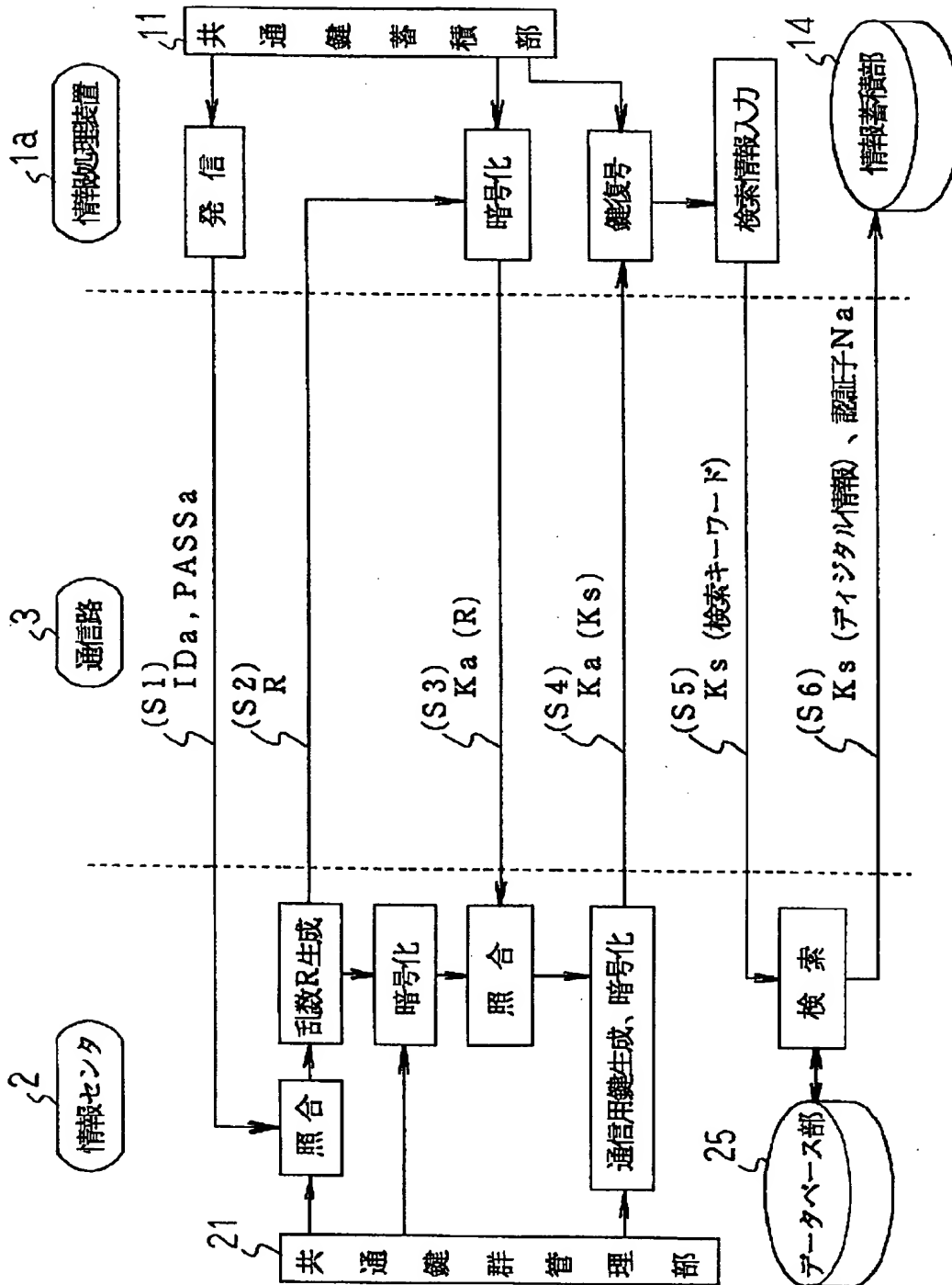
【図3】

IDa	PASSa	Ka
IDb	PASSb	Kb
IDc	PASSc	Kc
...

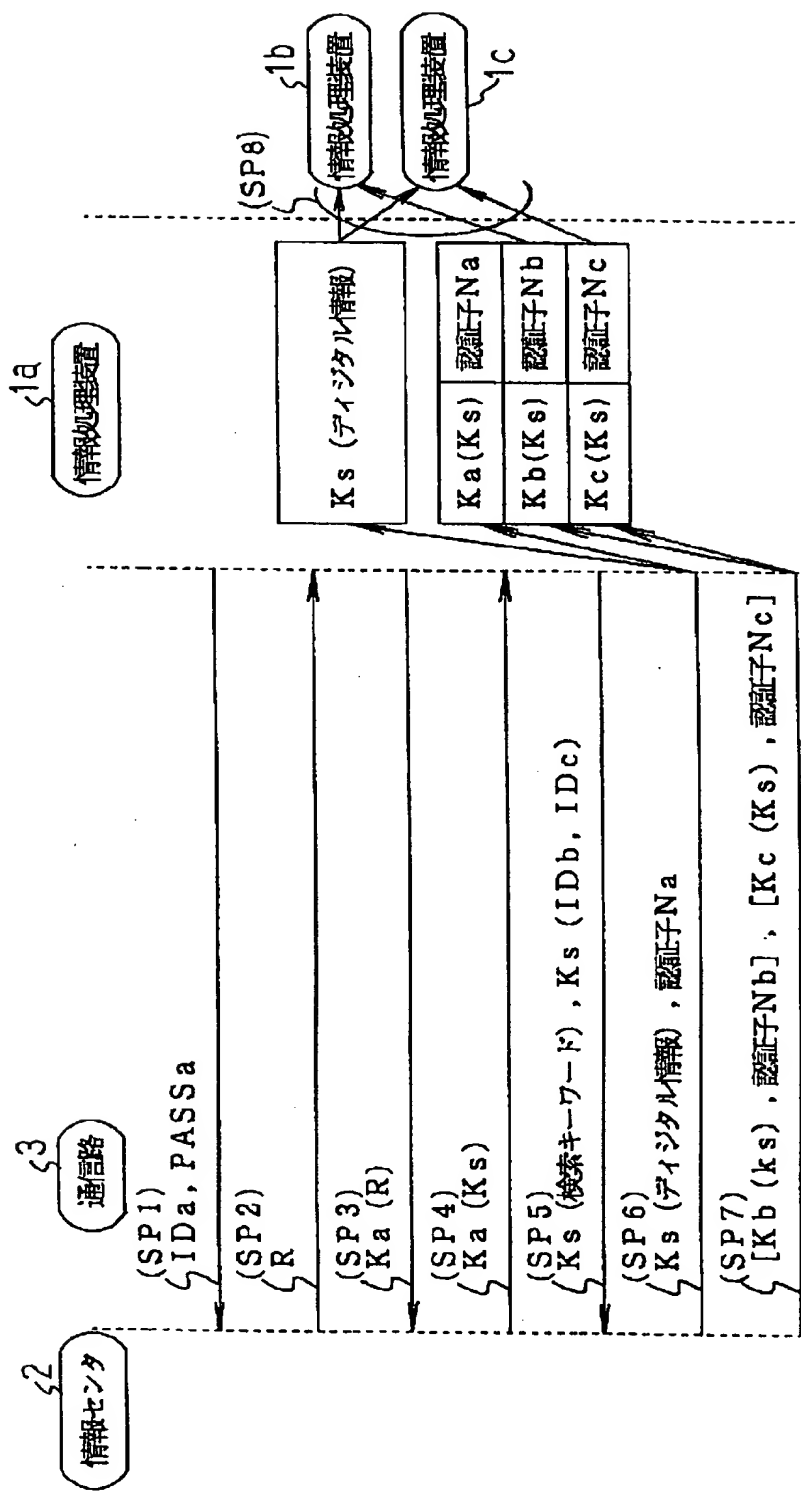
【図 1】



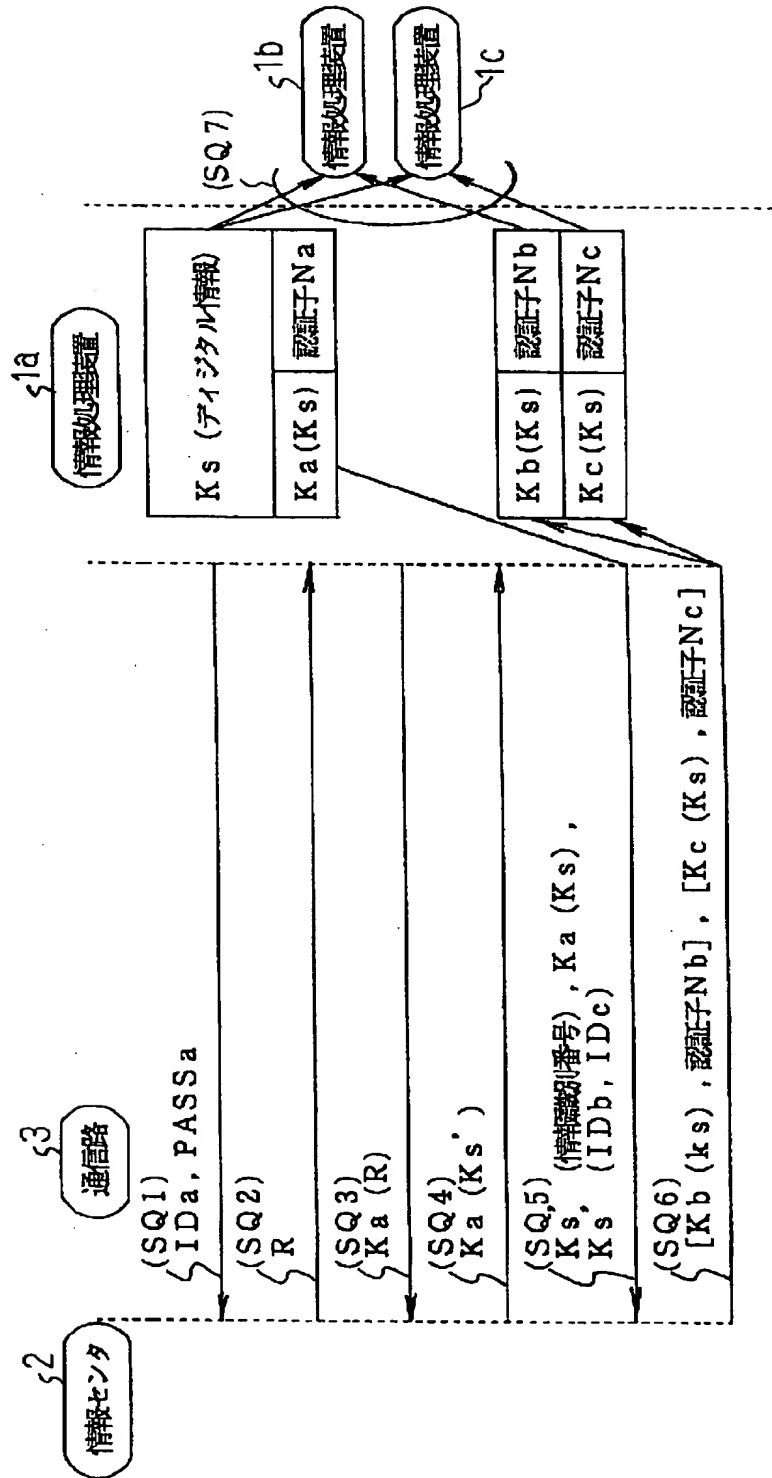
【図4】



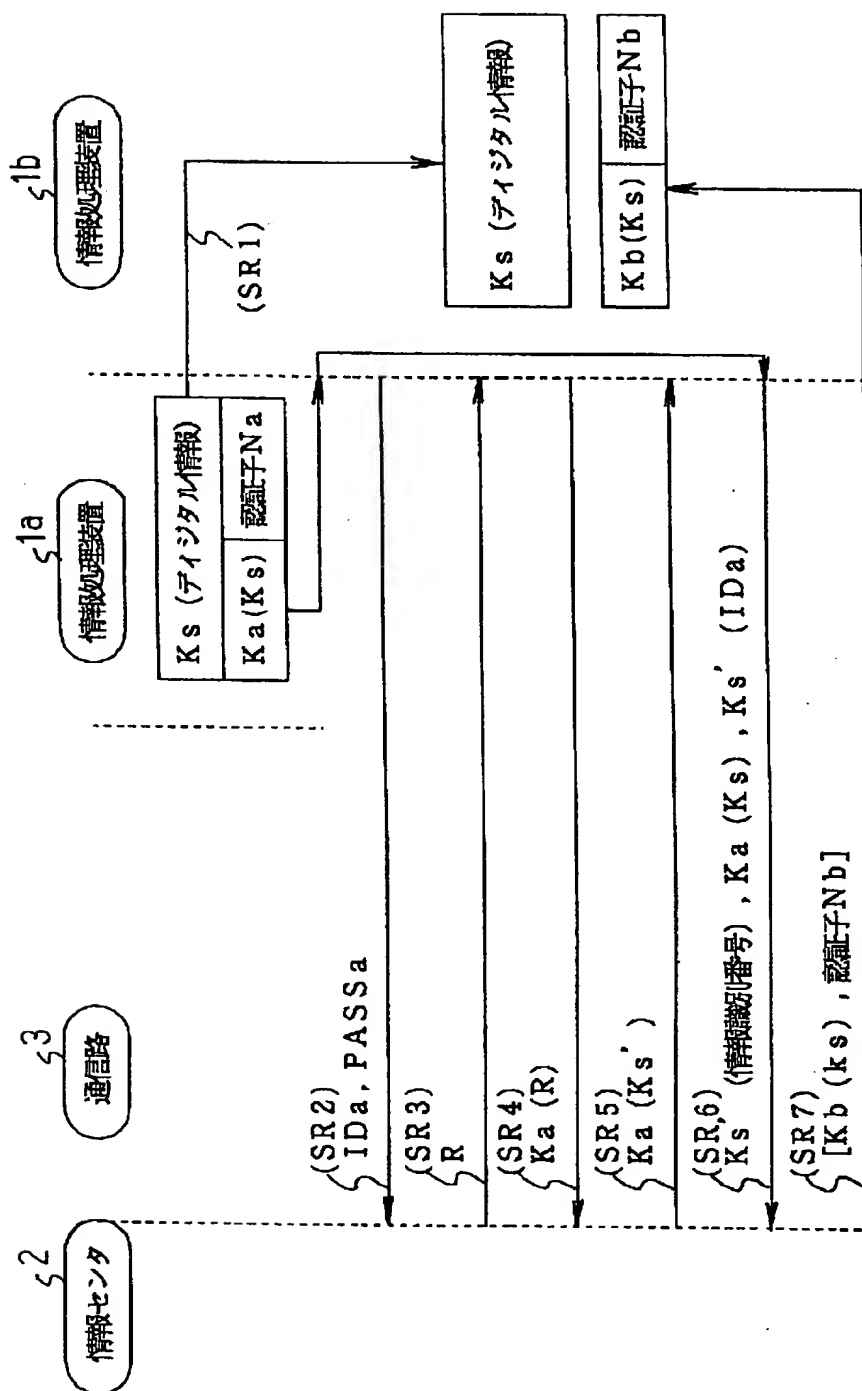
【図 5】



【図 6】



【図 7】



フロントページの続き

(51)Int.Cl.⁶
G 0 9 C 1/00

識別記号

庁内整理番号
9364-5L

F I

技術表示箇所